

## REMARKS

Claims 1 to 14 are pending in the application.

### **Rejection under 35 U.S.C. 102**

Claims 1-14 stand rejected under 35 U.S.C. 102(b) as being anticipated by *Craig* (US 6,266,809).

The present invention in amended claim 1 claims a method for performing an update of a program in a program-controlled device, wherein the method comprises the steps of:

connecting the program-controlled device (1) to an external Web browser (5), wherein the program-controlled device (1) comprises Web server functions for communicating with the external Web browser (5) and a network connector for accessing a Web server (2);

causing the device (1), initiated by the external Web browser (5), to request update information for an update of a program of the program-controlled device (1) from the Web server (2);

downloading the requested update information from the Web server (2) to the external Web browser (5), wherein the requested update information is being passed through the program-controlled device (1) to the external Web browser (5);

caching the requested update information by a program code executed in the external Web browser (5); and

programming the requested update information into the program-controlled device (1) by the program code executed in the external Web browser (5).

The program-controlled device according to the invention comprises:

a network connector for providing a connection to a Web server (2);

an interface for providing a connection with an external Web browser (5);

Web server functions enabling, upon request by the external Web browser (5) connected through the interface, downloading of update information from the Web server (2) connected through the network connector and transferring of the update information to the connected external Web browser (5);

a stored program code (6) executable in the connected external Web browser (5); and

at least one program changeable by the program code executable in the connected external Web browser with the update information transferred to the external Web browser (5).

The claims have been amended to include the term “external” Web browser in order to clarify that the Web browser is not part of the program-controlled device. Even though “external” is not explicitly used in the specification, it is apparent from the specification and the drawings that the device 1 and the computer 4 where the Web browser is installed are separate devices (see paragraph 0035; Figure).

As explained in detail in paragraphs 0038 to 0041 of the instant specification, via the Web browser a command for an update is triggered and transferred to the device which in turn contacts the Web server and requests an update. The update passes through the device to the Web browser where it is cached by Java applet. The Java applet is started within the Web browser and the update information is then programmed by Java applet into the device; these steps are shown in the Figure by arrows a) through e). It is apparent that the device is a “transfer station” between the Web browser and the Web server (arrows a) and b) to request an update; arrows c) and d) to download an update to the Web browser) before the update is installed in the last step e) in the device.

The *Craig* reference shows a different configuration and different method. The environment is that of a server and network computers. Network computers (see col. 2, lines 3-7) are diskless computers that have no persistent storage and due to the lack of storage/disk, all programs and data - except the small loading program - are obtained from the server. See also col. 3, lines 7 to 23, where the special situation of network computers and the relation to the server are discussed. It is the server that holds all programs while the network computers only have firmware or device drivers.

The *Craig* reference deals with such a firmware update on network computers. The method is described in particular in connection with Figs. 4A and 4B; see col. 7, line 1, to col. 8, line 13. The method of *Craig* is based on the **server triggering an update of the firmware in the network computer** in that the server compares the installed firmware with the revision code, for example. When the server determines that the network computer requires an update, the network computer is shut down by the server and rebooted with the operating system provided by the server and including the update. The update is

downloaded onto the network computer and the update is installed (compare col. 7, lines 22-28; lines 55-61). After the update has been installed successfully, the network computer reboots with the regular operating system of the server (col. 7, lines 58-63).

Thus, the **control of the update resides exclusively in the server**; there is no other way of triggering an update and the network computer is controlled completely by the server operation. See also language of claim 1 of *Craig*; the first step reads: “detecting, at the network server, whether the network computer firmware is to be updated”.

In contrast to the configuration and method of *Craig*, the present invention is based on three essential components: a device that is to receive an update; a server that makes available the update; and a Web browser that is located on any external (even a remote location) device (computer) and through which an update is initiated. The present invention is not server-controlled but user-controlled: The user him/herself is to decide when an update and which update should be carried out. The user therefore maintains control over his device instead of the server taking over as it pleases. The use of a Web browser as a user interface also enables the user to access the device from a remote location.

*Craig* neither discloses a Web browser that sends a command to the Web server through the device for initiating an update nor discloses a step of intermediate storage by a program code (especially a Java applet) that is executed in the Web browser. Even though the reference refers to a Web browser (col. 1, lines 61ff) and to the use of Java as a runtime environment and programming language (col. 2, lines 32-35) as being known in general, there is no suggestion to use Java applets in a Web browser for caching the update and programming the update information in the device. The procedure that is disclosed in *Craig* is designed for the special situation of a server/network computer system. There is no external Web browser that sends a command for an update to a Web server through the device to be updated; there is also no step of caching the update by a program code such as a Java applet and programming the update in the device by the Java applet.

Claims 1 and 8 and their dependent claims are therefore not anticipated or obvious in view of the cited reference.

In regard to claim 12, the examiner states that *Craig* discloses a program code that is executable in a Web browser as evidenced by the disclosure of col. 6, lines 20-35. There

is no mention of a Web browser in the cited passage. The examiner further refers to cache being disclosed in col. 5, lines 30-37; however, this passage states only that a cache is used but not that a program code executable in the Web browser is caching the update information. The reference also does not disclose in col. 7, lines 30-45, that a program code executable in a Web browser programs the update into the device. In particular, there is no disclosure that the program code that caches the update in the Web browser and programs the update into the device could be a Java applet as claimed in claim 13.

Claim 12 and its dependent claims are therefore not anticipated by *Craig*.

### **CONCLUSION**

In view of the foregoing, it is submitted that this application is now in condition for allowance and such allowance is respectfully solicited.

Should the Examiner have any further objections or suggestions, the undersigned would appreciate a phone call or **e-mail** from the examiner to discuss appropriate amendments to place the application into condition for allowance.

Authorization is herewith given to charge any fees or any shortages in any fees required during prosecution of this application and not paid by other means to Patent and Trademark Office deposit account 50-1199.

Respectfully submitted on June 19, 2007,

/Gudrun E. Hockett/

---

Ms. Gudrun E. Hockett, Ph.D.  
Patent Agent, Registration No. 35,747  
Schubertstr. 15a  
42289 Wuppertal  
GERMANY  
Telephone: +49-202-257-0371  
Facsimile: +49-202-257-0372  
gudrun.draudt@t-online.de

GEH